PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-229447
(43)Date of publication of application : 14.08.2002

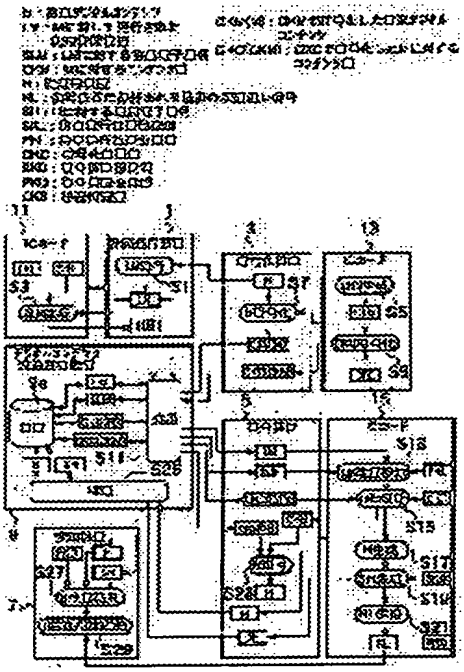
(51)Int.Cl. G09C 1/00
G06F 12/14
G06K 17/00
G06K 19/10
H04L 9/08

(21)Application number : 2001-022179
(22)Date of filing : 30.01.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MATSUOKA HISANOBU
HORI MASAHIRO

(54) COPYRIGHT PROTECTION SYSTEM IN DIGITAL CONTENTS DISTRIBUTION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a copyright protection system in a digital contents distribution which detects that digital contents are illegally used beyond a licensed range determined by use license information issued to the digital contents and prevents th illegal use.
SOLUTION: A license issuing device 1 issues use license information LM which defines a licensed range for digital contents M, and creates a licensed electronic signature SLM for use license information LM in an IC card 11 for the license issuing device with the secret key SKL of the license issuing device. A decoder 5 decodes the digital contents M encrypted with a contents key CKM in an encryption device 3 in an IC card 15 for the decoder according to the licensed range defined by the use license information LM, and detects the illegal tampering of use license information LM in the IC card 15 for the decoder by using the public key PKL and the license electronic signature SLM of the license issuing device which are shared with the license issuing device 1.



LEGAL STATUS

[Date of request for examination] 29.05.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Dat of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－229447
（P2002－229447A）
(43)公開日　平成14年８月14日(2002.8.14)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ　５Ｂ０１７
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｚ　５Ｂ０３５
	３２０		３２０Ｂ　５Ｂ０５８
			３２０Ｅ　５Ｊ１０４
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ

審査請求　有　　請求項の数14　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願2001－22179(P2001－22179)

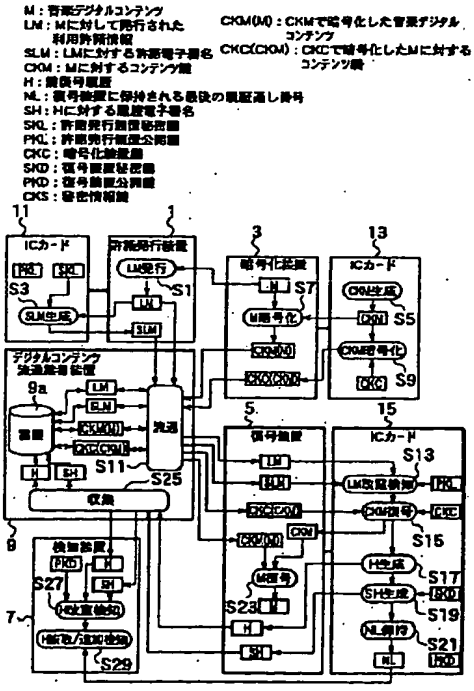
(22)出願日　平成13年１月30日(2001.1.30)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　松岡　寿延
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　堀　正弘
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】　デジタルコンテンツ流通における著作権保護システム

(57)【要約】
【課題】　デジタルコンテンツに対して発行された利用許諾情報の定める許諾範囲を逸脱してデジタルコンテンツが不正に利用されることを検知して防止するデジタルコンテンツ流通における著作権保護システムを提供する。
【解決手段】　許諾発行装置１はデジタルコンテンツＭに対して許諾範囲を定義した利用許諾情報ＬＭを発行し、許諾発行装置秘密鍵ＳＫＬで利用許諾情報ＬＭに対する許諾電子署名ＳＬＭを許諾発行装置用ＩＣカード１１内で生成し、復号装置５は暗号化装置３においてコンテンツ鍵ＣＫＭで暗号化されたデジタルコンテンツＭを利用許諾情報ＬＭの定義する許諾範囲に従って復号装置用ＩＣカード１５内で復号するとともに、許諾発行装置１と共有する許諾発行装置公開鍵ＰＫＬおよび許諾電子署名ＳＬＭにより利用許諾情報ＬＭの不正改竄を復号装置用ＩＣカード１５内で検知する。



1

【特許請求の範囲】

【請求項１】　流通するデジタルコンテンツの不正利用を防止するデジタルコンテンツ流通における著作権保護システムであって、

デジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行する許諾発行装置であって、当該許諾発行装置に固有の許諾発行装置秘密鍵を保持している許諾発行装置秘密鍵保持手段、およびこの保持している許諾発行装置秘密鍵で前記利用許諾情報に対する許諾電子署名を生成して該利用許諾情報に付加する許諾電子署名生成付与手段を有する許諾発行装置と、

前記デジタルコンテンツに固有のコンテンツ鍵でデジタルコンテンツを暗号化する暗号化装置と、

前記許諾発行装置と共有する許諾発行装置公開鍵を保持する鍵保持手段、この保持している許諾発行装置公開鍵および前記利用許諾情報に付加された許諾電子署名により該利用許諾情報の不正改竄を検知する不正改竄検知手段、および前記コンテンツ鍵で暗号化されたデジタルコンテンツを前記利用許諾情報の定義する許諾範囲に従って復号するコンテンツ復号手段を有する復号装置とを有することを特徴とするデジタルコンテンツ流通における著作権保護システム。

【請求項２】　前記暗号化装置は、

前記デジタルコンテンツに固有のコンテンツ鍵を生成するコンテンツ鍵生成手段、暗号化装置鍵を保持している暗号化装置鍵保持手段、およびこの保持している暗号化装置鍵で前記コンテンツ鍵を暗号化するコンテンツ鍵暗号化手段を更に有し、

前記復号装置の前記鍵保持手段が当該復号装置に固有の復号装置秘密鍵、前記暗号化装置と共有する暗号化装置鍵を更に保持しており、

前記復号装置は、

前記暗号化装置鍵で暗号化されたコンテンツ鍵を前記暗号化装置と共有する暗号化装置鍵で復号するコンテンツ鍵復号手段、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成する鍵復号履歴生成手段、前記履歴通し番号を保持する履歴通し番号保持手段、および前記鍵保持手段に保持している復号装置秘密鍵で前記鍵復号履歴に履歴電子署名を付加する履歴電子署名付加手段を更に有することを特徴とする請求項１記載のデジタルコンテンツ流通における著作権保護システム。

【請求項３】　前記復号装置と共有する復号装置公開鍵および前記鍵復号履歴に付加された履歴電子署名により前記鍵復号履歴の不正改竄を検知する鍵復号履歴不正改竄検知手段、および前記鍵復号履歴に含まれる履歴通し番号の連続性および前記復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知する不正抜取／追加検知手段を有する検知装置を更に有することを特徴とする請求項２記載のデジタルコンテンツ流通における著作権保護システム。

2

【請求項４】　流通するデジタルコンテンツの不正利用を防止するデジタルコンテンツ流通における著作権保護システムであって、

デジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行する許諾発行装置であって、当該許諾発行装置に固有の許諾発行装置秘密鍵を保持している許諾発行装置秘密鍵保持手段、およびこの保持している許諾発行装置秘密鍵で前記利用許諾情報に対する許諾電子署名を生成して該利用許諾情報に付加する許諾電子署名生成手段を有する許諾発行装置と、

前記デジタルコンテンツに固有のコンテンツ鍵を生成するコンテンツ鍵生成手段、該コンテンツ鍵で前記デジタルコンテンツを暗号化するコンテンツ暗号化手段、暗号化装置鍵を保持している暗号化装置鍵保持手段、およびこの保持している暗号化装置鍵で前記コンテンツ鍵を暗号化するコンテンツ鍵暗号化手段を有する暗号化装置と、

前記許諾発行装置と共有する許諾発行装置公開鍵、復号装置に固有の復号装置秘密鍵、前記暗号化装置と共有する暗号化装置鍵を保持する鍵保持手段、この保持している許諾発行装置公開鍵および前記利用許諾情報に付加された許諾電子署名により該利用許諾情報の不正改竄を検知する利用許諾情報不正改竄検知手段、前記暗号化装置鍵で暗号化されたコンテンツ鍵を前記鍵保持手段に保持している暗号化装置鍵で復号するコンテンツ鍵復号手段、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成する鍵復号履歴生成手段、前記履歴通し番号を保持する履歴通し番号保持手段、前記保持している復号装置秘密鍵で前記鍵復号履歴に履歴電子署名を付加する履歴電子署名付加手段、および前記復号されたコンテンツ鍵を用いて、前記コンテンツ鍵で暗号化されたデジタルコンテンツを前記利用許諾情報の定義する許諾範囲に従って復号するコンテンツ復号手段を有する復号装置と、

前記復号装置と共有する復号装置公開鍵および前記鍵復号履歴に付加された履歴電子署名により前記鍵復号履歴の不正改竄を検知する鍵復号履歴不正改竄検知手段、および前記鍵復号履歴に含まれる履歴通し番号の連続性および前記復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知する不正抜取／追加検知手段を有する検知装置とを有することを特徴とするデジタルコンテンツ流通における著作権保護システム。

【請求項５】　前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行することを特徴とする請求項４記載のデジタ

ルコンテンツ流通における著作権保護システム。

【請求項６】　前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行することを特徴とする請求項４記載のデジタルコンテンツ流通における著作権保護システム。

【請求項７】　前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行することを特徴とする請求項４記載のデジタルコンテンツ流通における著作権保護システム。

【請求項８】　前記暗号化装置、許諾発行装置、および復号装置は、秘密情報鍵を共有し、

前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、

前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有し、

前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを特徴とする請求項４記載のデジタルコンテンツ流通における著作権保護システム。

【請求項９】　前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、

前記許諾発行装置および復号装置は、秘密情報鍵を共有し、

前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有し、

前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを特徴とする請求項４記載のデジタルコンテンツ流通における著作権保護システム。

【請求項１０】　前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持手段および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行し、

前記暗号化装置および復号装置は、秘密情報鍵を共有し、

前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、

前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを特徴とする請求項４記載のデジタルコンテンツ流通における著作権保護システム。

【請求項１１】　前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行し、

前記暗号化装置および許諾発行装置は、秘密情報鍵を共有し、

前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、

前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有することを特徴とする請求項４記載のデジタルコンテンツ流通における著作権保護システム。

【請求項１２】　前記暗号化装置は、暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、

前記許諾発行装置の前記許諾発行装置秘密鍵保持手段および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行し、

前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行することを特徴とする請求項４記載のデジタルコンテンツ流通における著作権保護システム。

【請求項１３】　前記許諾発行装置は、前記許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持する手段を有し、

前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、

前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署

5

名付加をタンパフリー性ハードウェア内に閉じて実行することを特徴とする請求項４記載のデジタルコンテンツ流通における著作権保護システム。

【請求項１４】　前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有し、

前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、

前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行することを特徴とする請求項４記載のデジタルコンテンツ流通における著作権保護システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、流通するデジタルコンテンツの不正利用を防止するデジタルコンテンツ流通における著作権保護システムに関し、詳しくは、ネットワークまたはデジタル記録媒体を介して流通するデジタルコンテンツが当該コンテンツに対して発行された利用許諾情報の定める許諾範囲を逸脱して不正に利用されることを検知して防止するデジタルコンテンツ流通における著作権保護システムに関する。

【０００２】

【従来の技術】デジタルコンテンツ流通サービスにおいては、デジタルコンテンツの複製の容易性のため、デジタルコンテンツに対して定められた許諾範囲を逸脱した不正利用を検知して防止する技術が必須である。この技術は、具体的には以下に記載する２つの技術から構成される。

【０００３】すなわち、第１の技術は、デジタルコンテンツの許諾範囲を定める利用許諾情報の改竄を検知する技術およびこの許諾範囲を逸脱する不正利用を防止する技術であり、第２の技術は、デジタルコンテンツの利用時の利用履歴生成および利用履歴検証による不正利用の検知技術である。

【０００４】

【発明が解決しようとする課題】上述した技術のうち、第１の技術においては、デジタルコンテンツに利用許諾情報を付随する場合には、この利用許諾情報の不正改竄による不正利用という問題があり、また利用許諾情報をセンタで管理する場合には、ネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という問題がある。

【０００５】また、第２の技術においては、利用履歴の

6

改竄や抜き取りによる不正利用という問題があることに加えて、この利用履歴をセンタで管理する場合には、ネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という問題がある。

【０００６】本発明は、上記に鑑みてなされたもので、その目的とするところは、デジタルコンテンツに対して発行された利用許諾情報の定める許諾範囲を逸脱してデジタルコンテンツが不正に利用されることを検知して防止するデジタルコンテンツ流通における著作権保護システムを提供することにある。

【０００７】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、流通するデジタルコンテンツの不正利用を防止するデジタルコンテンツ流通における著作権保護システムであって、デジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行する許諾発行装置であって、当該許諾発行装置に固有の許諾発行装置秘密鍵を保持している許諾発行装置秘密鍵保持手段、およびこの保持している許諾発行装置秘密鍵で前記利用許諾情報に対する許諾電子署名を生成して該利用許諾情報に付加する許諾電子署名生成付与手段を有する許諾発行装置と、前記デジタルコンテンツに固有のコンテンツ鍵でデジタルコンテンツを暗号化する暗号化装置と、前記許諾発行装置と共有する許諾発行装置公開鍵を保持する鍵保持手段、この保持している許諾発行装置公開鍵および前記利用許諾情報に付加された許諾電子署名により該利用許諾情報の不正改竄を検知する不正改竄検知手段、および前記コンテンツ鍵で暗号化されたデジタルコンテンツを前記利用許諾情報の定義する許諾範囲に従って復号するコンテンツ復号手段を有する復号装置とを有することを要旨とする。

【０００８】請求項１記載の本発明にあっては、許諾発行装置はデジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行し、許諾発行装置に固有の許諾発行装置秘密鍵で利用許諾情報に対する許諾電子署名を生成し、復号装置は暗号化装置においてコンテンツ鍵で暗号化されたデジタルコンテンツを利用許諾情報の定義する許諾範囲に従って復号するとともに、許諾発行装置と共有する許諾発行装置公開鍵および許諾電子署名により利用許諾情報の不正改竄を検知するため、デジタルコンテンツを許諾範囲内のみで利用可能とし、許諾範囲を逸脱した不正利用を検知して防止することができ、またネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という従来の問題を解決できる。また、復号装置は復号時に許諾発行装置などの外部と接続されている必要がない。

【０００９】また、請求項２記載の本発明は、請求項１記載の発明において、前記暗号化装置が、前記デジタル

7

コンテンツに固有のコンテンツ鍵を生成するコンテンツ鍵生成手段、暗号化装置鍵を保持している暗号化装置鍵保持手段、およびこの保持している暗号化装置鍵で前記コンテンツ鍵を暗号化するコンテンツ鍵暗号化手段を更に有し、前記復号装置の前記鍵保持手段が当該復号装置に固有の復号装置秘密鍵、前記暗号化装置と共有する暗号化装置鍵を更に保持しており、前記復号装置は、前記保持されている暗号化装置鍵で暗号化されたコンテンツ鍵を前記暗号化装置と共有する暗号化装置鍵で復号するコンテンツ鍵復号手段、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成する鍵復号履歴生成手段、前記履歴通し番号を保持する履歴通し番号保持手段、および前記鍵保持手段に保持している復号装置秘密鍵で前記鍵復号履歴に履歴電子署名を付加する履歴電子署名付加手段を更に有することを要旨とする。

【００１０】請求項２記載の本発明にあっては、暗号化装置はデジタルコンテンツに固有のコンテンツ鍵を生成し、暗号化装置鍵でコンテンツ鍵を暗号化し、復号装置は暗号化されたコンテンツ鍵を暗号化装置鍵で復号し、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成し、履歴通し番号を保持し、復号装置秘密鍵で鍵復号履歴に履歴電子署名を付加する。

【００１１】更に、請求項３記載の本発明は、請求項２記載の発明において、前記復号装置と共有する復号装置公開鍵および前記鍵復号履歴に付加された履歴電子署名により前記鍵復号履歴の不正改竄を検知する鍵復号履歴不正改竄検知手段、および前記鍵復号履歴に含まれる履歴通し番号の連続性および前記復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知する不正抜取／追加検知手段を有する検知装置を更に有することを要旨とする。

【００１２】請求項３記載の本発明にあっては、検知装置は復号装置公開鍵および鍵復号履歴に付加された履歴電子署名により鍵復号履歴の不正改竄を検知し、鍵復号履歴に含まれる履歴通し番号の連続性および復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知するため、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができる。また、検知装置による鍵復号履歴の収集は復号時である必要はなく、復号装置は復号時に検知装置に接続されている必要がない。

【００１３】請求項４記載の本発明は、流通するデジタルコンテンツの不正利用を防止するデジタルコンテンツ流通における著作権保護システムであって、デジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行する許諾発行装置であって、当該許諾発行装置に固有の許諾発行装置秘密鍵を保持している許諾発行装置秘密鍵保持手段、およびこの保持している許諾発行装置秘密鍵で前記利用許諾情報に対する許諾電子署名を生成して

8

該利用許諾情報に付加する許諾電子署名生成手段を有する許諾発行装置と、前記デジタルコンテンツに固有のコンテンツ鍵を生成するコンテンツ鍵生成手段、該コンテンツ鍵で前記デジタルコンテンツを暗号化するコンテンツ暗号化手段、暗号化装置鍵を保持している暗号化装置鍵保持手段、およびこの保持している暗号化装置鍵で前記コンテンツ鍵を暗号化するコンテンツ鍵暗号化手段を有する暗号化装置と、前記許諾発行装置と共有する許諾発行装置公開鍵、復号装置に固有の復号装置秘密鍵、前記暗号化装置と共有する暗号化装置鍵を保持する鍵保持手段、この保持している許諾発行装置公開鍵および前記利用許諾情報に付加された許諾電子署名により該利用許諾情報の不正改竄を検知する利用許諾情報不正改竄検知手段、前記暗号化装置鍵で暗号化されたコンテンツ鍵を前記鍵保持手段に保持している暗号化装置鍵で復号するコンテンツ鍵復号手段、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成する鍵復号履歴生成手段、前記履歴通し番号を保持する履歴通し番号保持手段、前記保持している復号装置秘密鍵で前記鍵復号履歴に履歴電子署名を付加する履歴電子署名付加手段、および前記復号されたコンテンツ鍵を用いて、前記コンテンツ鍵で暗号化されたデジタルコンテンツを前記利用許諾情報の定義する許諾範囲に従って復号するコンテンツ復号手段を有する復号装置と、前記復号装置と共有する復号装置公開鍵および前記鍵復号履歴に付加された履歴電子署名により前記鍵復号履歴の不正改竄を検知する鍵復号履歴不正改竄検知手段、および前記鍵復号履歴に含まれる履歴通し番号の連続性および前記復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知する不正抜取／追加検知手段とを有することを要旨とする。

【００１４】請求項４記載の本発明にあっては、許諾発行装置はデジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行し、許諾発行装置秘密鍵で利用許諾情報に対する許諾電子署名を生成し、暗号化装置はデジタルコンテンツに固有のコンテンツ鍵を生成し、該コンテンツ鍵でデジタルコンテンツを暗号化し、暗号化装置鍵でコンテンツ鍵を暗号化し、復号装置は許諾発行装置公開鍵および利用許諾情報に付加された許諾電子署名により利用許諾情報の不正改竄を検知し、暗号化されたコンテンツ鍵を暗号化装置鍵で復号し、この復号時に連続した自然数を履歴通し番号として含む鍵復号履歴を生成し、履歴通し番号を保持し、復号装置秘密鍵で鍵復号履歴に履歴電子署名を付加し、暗号化されたデジタルコンテンツをコンテンツ鍵で利用許諾情報の定義する許諾範囲に従って復号し、検知装置は復号装置公開鍵および鍵復号履歴に付加された履歴電子署名により鍵復号履歴の不正改竄を検知し、鍵復号履歴に含まれる履歴通し番号の連続性および復号装置に保持している履歴通し番号

の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知するため、デジタルコンテンツを許諾範囲内のみで利用可能とし、許諾範囲を逸脱した不正利用を検知して防止することができ、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができるとともに、コンテンツ利用後の利用履歴抜き取りまたは改竄によるデジタルコンテンツの不正利用を検知して防止でき、またネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という従来の問題を解決できる。

【００１５】また、請求項５記載の本発明は、請求項４記載の発明において、前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行することを要旨とする。

【００１６】請求項５記載の本発明にあっては、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリー性ハードウェア内に閉じて実行するため、暗号化装置のセキュリティを高め、その不正防止効果を向上することができる。

【００１７】更に、請求項６記載の本発明は、請求項４記載の発明において、前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行することを要旨とする。

【００１８】請求項６記載の本発明にあっては、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与をタンパフリー性ハードウェア内に閉じて実行するため、許諾発行装置のセキュリティを高め、その不正防止効果を向上することができる。

【００１９】請求項７記載の本発明は、請求項４記載の発明において、前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行することを要旨とする。

【００２０】請求項７記載の本発明にあっては、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行するため、復号装置のセキュリティを高め、その不正防止効果を向上することができる。

【００２１】また、請求項８記載の本発明は、請求項４記載の発明において、前記暗号化装置、許諾発行装置、および復号装置は、秘密情報鍵を共有し、前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを要旨とする。

【００２２】請求項８記載の本発明にあっては、暗号化装置、許諾発行装置、および復号装置は、秘密情報鍵を共有し、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００２３】更に、請求項９記載の本発明は、請求項４記載の発明において、前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、前記許諾発行装置および復号装置は、秘密情報鍵を共有し、前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記復号装置は、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを要旨とする。

【００２４】請求項９記載の本発明にあっては、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリー性ハードウェア内に閉じて実行し、許諾発行装置および復号装置は秘密情報鍵を共有し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００２５】請求項１０記載の本発明は、請求項４記載の発明において、前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持手段および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行し、前記暗号化装置および復号装置は、秘密情報鍵を共有し、前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記復号装置は、前記暗号化

装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有することを要旨とする。

【００２６】請求項１０記載の本発明にあっては、許諾発行装置は許諾発行装置秘密鍵保持手段および許諾電子署名生成付与をタンパフリー性ハードウェア内に閉じて実行し、暗号化装置および復号装置は秘密情報鍵を共有し、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００２７】請求項１１記載の本発明は、請求項４記載の発明において、前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行し、前記暗号化装置および許諾発行装置は、秘密情報鍵を共有し、前記暗号化装置は、前記暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記許諾発行装置は、前記許諾発行装置秘密鍵を前記秘密情報鍵で暗号化して保持する手段を有することを要旨とする。

【００２８】請求項１１記載の本発明にあっては、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行し、暗号化装置および許諾発行装置は秘密情報鍵を共有し、暗号化装置は暗号化装置鍵を前記秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００２９】更に、請求項１２記載の本発明は、請求項４記載の発明において、前記暗号化装置は、暗号化装置鍵を前記秘密情報鍵で暗号化して保持する手段を有し、前記許諾発行装置の前記許諾発行装置秘密鍵保持手段および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行し、前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行することを要旨とする。

【００３０】請求項１２記載の本発明にあっては、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行し、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００３１】請求項１３記載の本発明は、請求項４記載の発明において、前記許諾発行装置は、前記許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持する手段を有し、前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、前記復号装置の前記鍵保持手段、前記利用許諾情報不正改竄検知手段、前記コンテンツ鍵復号手段、前記鍵復号履歴生成手段、前記履歴通し番号保持手段、前記履歴電子署名付加手段をタンパフリー性ハードウェアで構成し、鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行することを要旨とする。

【００３２】請求項１３記載の本発明にあっては、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００３３】また、請求項１４記載の本発明は、請求項４記載の発明において、前記復号装置が、前記暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持する手段を有し、前記暗号化装置の前記コンテンツ鍵生成手段、前記コンテンツ鍵暗号化手段、および前記暗号化装置鍵保持手段をタンパフリー性ハードウェアで構成し、コンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、前記許諾発行装置の前記許諾発行装置秘密鍵保持手段、および前記許諾電子署名生成付与手段をタンパフリー性ハードウェアで構成

し、許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行することを要旨とする。

【００３４】請求項１４記載の本発明にあっては、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を前記秘密情報鍵で暗号化して保持し、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持を前記タンパフリー性ハードウェア内に閉じて実行し、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与を前記タンパフリー性ハードウェア内に閉じて実行するため、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００３５】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。図１は、本発明の一実施形態に係るデジタルコンテンツ流通における著作権保護システムの構成を示す図である。同図に示す著作権保護システムは、許諾発行装置用ＩＣカード１１が接続された許諾発行装置１、暗号化装置用ＩＣカード１３が接続された暗号化装置３、復号装置用ＩＣカード１５が接続された復号装置５、検知装置７、およびデジタルコンテンツ流通業者装置９から構成されている。

【００３６】許諾発行装置１および許諾発行装置用ＩＣカード１１は、互いにシリアルケーブルまたはＵＳＢケーブルなどの汎用的なインタフェースで接続され、例えば音楽デジタルコンテンツＭに対して許諾範囲を定義した利用許諾情報ＬＭを発行する利用許諾情報発行手段、当該許諾発行装置１に固有の許諾発行装置秘密鍵ＳＫＬおよび許諾発行装置公開鍵ＰＫＬを保持している許諾発行装置秘密鍵保持手段、およびこの保持している許諾発行装置秘密鍵ＳＫＬで利用許諾情報ＬＭに対する許諾電子署名ＳＬＭを生成して利用許諾情報ＬＭに付加する許諾電子署名生成手段を有し、これらの手段のうち、許諾発行装置秘密鍵保持手段および許諾電子署名生成付与手段をタンパフリー性ハードウェアである許諾発行装置用ＩＣカード１１で構成し、これにより許諾発行装置秘密鍵保持および許諾電子署名生成付与をタンパフリー性ハードウェアである許諾発行装置用ＩＣカード１１内に閉じて実行して、許諾発行装置のセキュリティを高め、その不正防止効果を向上している。

【００３７】また、暗号化装置３および暗号化装置用ＩＣカード１３は、互いにシリアルケーブルまたはＵＳＢケーブルなどの汎用的なインタフェースで接続され、デジタルコンテンツＭに固有のコンテンツ鍵ＣＫＭを生成するコンテンツ鍵生成手段、該コンテンツ鍵ＣＫＭでデジタルコンテンツＭを暗号化するコンテンツ暗号化手段、暗号化装置鍵ＣＫＣを保持している暗号化装置鍵保持手段、およびこの保持している暗号化装置鍵ＣＫＣでコンテンツ鍵ＣＫＭを暗号化するコンテンツ鍵暗号化手段を有し、この手段のうち、コンテンツ鍵生成手段、コンテンツ鍵暗号化手段、および暗号化装置鍵保持手段をタンパフリー性ハードウェアである暗号化装置用ＩＣカード１３で構成し、これによりコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリー性ハードウェアである暗号化装置用ＩＣカード１３内に閉じて実行して、暗号化装置のセキュリティを高め、その不正防止効果を向上している。

【００３８】更に、復号装置５および復号装置用ＩＣカード１５は、互いにシリアルケーブルまたはＵＳＢケーブルなどの汎用的なインタフェースで接続され、許諾発行装置１と共有する許諾発行装置公開鍵ＰＫＬ、復号装置５に固有の復号装置秘密鍵ＳＫＤ、暗号化装置３と共有する暗号化装置鍵ＣＫＣを保持する鍵保持手段、この保持している許諾発行装置公開鍵ＰＫＬおよび利用許諾情報ＬＭに付加された許諾電子署名ＳＬＭにより利用許諾情報ＬＭの不正改竄を検知する利用許諾情報不正改竄検知手段、暗号化装置鍵ＣＫＣで暗号化されたコンテンツ鍵ＣＫＭを鍵保持手段に保持している暗号化装置鍵ＣＫＣで復号するコンテンツ鍵復号手段、この復号時に連続した自然数を履歴通し番号ＮＬとして含む鍵復号履歴Ｈを生成する鍵復号履歴生成手段、履歴通し番号ＮＬを保持する履歴通し番号保持手段、前記保持している復号装置秘密鍵ＳＫＤで鍵復号履歴Ｈに履歴電子署名ＳＨを付加する履歴電子署名付加手段、および前記コンテンツ鍵ＣＫＭで暗号化されたデジタルコンテンツを前記復号されたコンテンツ鍵ＣＫＭで利用許諾情報ＬＭの定義する許諾範囲に従って復号するコンテンツ復号手段を有し、これらの手段のうち、鍵保持手段、利用許諾情報不正改竄検知手段、コンテンツ鍵復号手段、鍵復号履歴生成手段、履歴通し番号保持手段、履歴電子署名付加手段をタンパフリー性ハードウェアである復号装置用ＩＣカード１５で構成し、これにより鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェアである復号装置用ＩＣカード１５内に閉じて実行して、復号装置のセキュリティを高め、その不正防止効果を向上している。

【００３９】また、検知装置７は、復号装置５と共有する復号装置公開鍵ＰＫＤおよび鍵復号履歴Ｈに付加された履歴電子署名ＳＨにより鍵復号履歴Ｈの不正改竄を検知する鍵復号履歴不正改竄検知手段、および鍵復号履歴Ｈに含まれる履歴通し番号ＮＬの連続性および復号装置５に保持している履歴通し番号ＮＬの参照により鍵復号履歴Ｈの不正な抜き取りおよび不正な追加を検知する不正抜取／追加検知手段を有する。

【００４０】また、デジタルコンテンツ流通業者装置９は、許諾発行装置１からの利用許諾情報ＬＭおよび許諾電子署名ＳＬＭの収集、暗号化装置３からのコンテンツ鍵ＣＫＭで暗号化されたデジタルコンテンツＭ（すなわ

ち、ＣＫＭ（Ｍ））、暗号化装置鍵ＣＫＣで暗号化されたコンテンツ鍵ＣＫＭ（すなわち、ＣＫＣ（ＣＫＭ））の収集を行い、これらをデータベース９ａに格納するとともに、復号装置５に送信して流通させるとともに、また復号装置５からの鍵復号履歴Ｈおよび履歴電子署名ＳＨの収集を行い、これらをデータベース９ａに格納するとともに、検知装置７に配送するように構成されている。

【００４１】なお、許諾発行装置１からデジタルコンテンツ流通業者装置９への利用許諾情報ＬＭおよび許諾電子署名ＳＬＭの受け渡しは、ネットワーク上の通信またはフロッピー（登録商標）ディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【００４２】また、暗号化装置３から許諾発行装置１への利用許諾情報ＬＭの発行要求は、本実施形態ではネットワーク上の通信を用いて行われるものとする。

【００４３】暗号化装置３からデジタルコンテンツ流通業者装置９へのコンテンツ鍵ＣＫＭで暗号化されたデジタルコンテンツＭ（すなわち、ＣＫＭ（Ｍ））および暗号化装置鍵ＣＫＣで暗号化されたコンテンツ鍵ＣＫＭ（すなわち、ＣＫＣ（ＣＫＭ））の受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【００４４】また、デジタルコンテンツ流通業者装置９から復号装置５への利用許諾情報ＬＭ、許諾電子署名ＳＬＭ、暗号化装置鍵ＣＫＣで暗号化されたコンテンツ鍵ＣＫＭ（すなわち、ＣＫＣ（ＣＫＭ））、およびコンテンツ鍵ＣＫＭで暗号化されたコンテンツＭ（すなわち、ＣＫＭ（Ｍ））の受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【００４５】更に、復号装置５からデジタルコンテンツ流通業者装置９への鍵復号履歴Ｈおよび履歴電子署名ＳＨの受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【００４６】デジタルコンテンツ通信業者装置９から検知装置７への鍵復号履歴Ｈおよび履歴電子署名ＳＨの受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【００４７】次に、以上のように構成される本実施形態のデジタルコンテンツ流通における著作権保護システムの作用について図１内に示すステップ番号Ｓ１～Ｓ２９を参照して説明する。

【００４８】まず、許諾発行装置１は、暗号化装置３からの音楽デジタルコンテンツＭに対する利用許諾情報ＬＭの発行要求に応答して該利用許諾情報ＬＭを発行する（ステップＳ１）。それから、許諾発行装置１に接続された許諾発行装置用ＩＣカード１１は、当該ＩＣカード１１内において許諾発行装置秘密鍵ＳＫＬを用いて、利用許諾情報ＬＭに対する許諾電子署名ＳＬＭを生成する（ステップＳ３）。

【００４９】次に、暗号化装置用ＩＣカード１３は、当該ＩＣカード１３内において前記デジタルコンテンツＭに固有のコンテンツ鍵ＣＫＭを生成する（ステップＳ５）。それから、暗号化装置３は、このコンテンツ鍵ＣＫＭを用いて、デジタルコンテンツＭを暗号化して、ＣＫＭ（Ｍ）を生成する（ステップＳ７）。また、暗号化装置用ＩＣカード１３は、当該ＩＣカード１３内において暗号化装置鍵ＣＫＣを用いて、前記コンテンツ鍵ＣＫＭを暗号化して、ＣＫＣ（ＣＫＭ）を生成する（ステップＳ９）。

【００５０】次に、デジタルコンテンツ流通業者装置９は、前記利用許諾情報ＬＭ、許諾電子署名ＳＬＭ、暗号化装置鍵ＣＫＣで暗号化されたコンテンツ鍵ＣＫＭであるＣＫＣ（ＣＫＭ）、コンテンツ鍵ＣＫＭで暗号化されたコンテンツＭであるＣＫＭ（Ｍ）を収集し、これらをネットワークを介して復号装置５に配送する（ステップＳ１１）。

【００５１】復号装置５に接続された復号装置用ＩＣカード１５は、当該ＩＣカード１５内において前記利用許諾情報ＬＭ、許諾電子署名ＳＬＭ、および許諾発行装置１と共有する許諾発行装置公開鍵ＰＫＬを用いて利用許諾情報ＬＭの改竄を検知する（ステップＳ１３）。この検知処理において利用許諾情報ＬＭの改竄が検知されない場合には、暗号化装置鍵ＣＫＣで暗号化されたコンテンツ鍵ＣＫＭであるＣＫＣ（ＣＫＭ）を暗号化装置鍵ＣＫＣで復号し、コンテンツ鍵ＣＫＭを生成する（ステップＳ１５）。そして、このコンテンツ鍵ＣＫＭの復号時に連続した自然数を履歴通し番号ＮＬとして含む鍵復号履歴Ｈを生成する（ステップＳ１７）。

【００５２】また、復号装置用ＩＣカード１５は、許諾発行装置に固有の復号装置秘密鍵ＳＫＤを用いて、前記鍵復号履歴Ｈに対する履歴電子署名ＳＨを生成し（ステップＳ１９）、更に鍵復号履歴Ｈに含まれている履歴通し番号ＮＬを最後の履歴通し番号ＮＬとして保持する（ステップＳ２１）。復号装置５は、コンテンツ鍵ＣＫＭで暗号化されたデジタルコンテンツＭであるＣＫＭ（Ｍ）をステップＳ１５で復号されたコンテンツ鍵ＣＫ

Mを用いて利用許諾情報ＬＭの定義する許諾範囲に従って復号して、デジタルコンテンツMを生成する（ステップＳ２３）。

【００５３】次に、デジタルコンテンツ流通業者装置９は、復号装置５から鍵復号履歴Ｈおよび履歴電子署名ＳＨを収集して、データベース９ａに格納する（ステップＳ２５）。

【００５４】それから、検知装置７は、デジタルコンテンツ流通業者装置９から受け取った鍵復号履歴Ｈおよび履歴電子署名ＳＨ、および復号装置５と共有している復号装置公開鍵ＰＫＤを用いて、鍵復号履歴Ｈの改竄を検知する（ステップＳ２７）。また、検知装置７は、鍵復号履歴Ｈおよびその前後の鍵復号履歴が含む履歴通し番号の連続性および復号装置５に保持している履歴通し番号ＮＬを参照して、鍵復号履歴Ｈの不正な抜き取りおよび不正な追加を検知する（ステップＳ２９）。

【００５５】上述したように、音楽デジタルコンテンツMを利用許諾情報ＬＭの定める許諾範囲内でのみ利用可能とし、この許諾範囲を逸脱したデジタルコンテンツMの不正利用を検知し、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができる音楽デジタルコンテンツ流通サービスを実現することができる。

【００５６】また、上記実施形態では、復号装置５は、復号時に許諾発行装置１などの外部と接続されている必要がないし、また検知装置７による鍵復号履歴Ｈの収集は復号時である必要はないため、復号装置５は復号時に検知装置７に接続されている必要もない。

【００５７】次に、図２を参照して、本発明の他の実施形態に係るデジタルコンテンツ流通における著作権保護システムについて説明する。

【００５８】図２に示す実施形態の著作権保護システムは、図１に示した実施形態における許諾発行装置１、暗号化装置３、および復号装置５をそれぞれ演算機能および記憶機能において分割して構成されるタンパフリー性ハードウェアを構成する許諾発行装置用ＩＣカード１１、暗号化装置用ＩＣカード１３、および復号装置用ＩＣカード１５を使用する代わりに、許諾発行装置、暗号化装置、および復号装置で共有する秘密情報鍵ＣＫＳを使用し、この秘密情報鍵ＣＫＳで許諾発行装置秘密鍵ＳＫＬ、暗号化装置鍵ＣＫＣ、復号装置秘密鍵ＳＫＤ、および履歴通し番号ＮＬを暗号化するように構成した点が異なるものであり、この構成および作用は図１の実施形態と同じである。

【００５９】すなわち、図２に示す著作権保護システムは、ＩＣカードでそれぞれ分割されていない許諾発行装置１０、暗号化装置３０および復号装置５０、検知装置７、およびデジタルコンテンツ流通業者装置９から構成されている。そして、許諾発行装置１０は、許諾発行装置秘密鍵ＳＫＬを秘密情報鍵ＣＫＳで暗号化したＣＫＳ（ＳＬＫ）を保持する手段を有し、暗号化装置３０は、暗号化装置鍵ＣＫＣを秘密情報鍵ＣＫＳで暗号化したＣＫＳ（ＣＫＣ）を保持する手段を有し、復号装置５０は、暗号化装置鍵ＣＫＣ、復号装置秘密鍵ＳＫＤ、履歴通し番号ＮＬを秘密情報鍵ＣＫＳで暗号化したＣＫＳ（ＣＫＣ）、ＣＫＳ（ＳＫＤ）、ＣＫＳ（ＮＬ）を保持する手段を有する。

【００６０】なお、許諾発行装置１０からデジタルコンテンツ流通業者装置９への利用許諾情報ＬＭおよび許諾電子署名ＳＬＭの受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【００６１】また、暗号化装置３０から許諾発行装置１０への利用許諾情報ＬＭの発行要求は、本実施形態ではネットワーク上の通信を用いて行われるものとする。

【００６２】暗号化装置３０からデジタルコンテンツ流通業者装置９へのコンテンツ鍵ＣＫＭで暗号化されたデジタルコンテンツMであるＣＫＭ（Ｍ）および暗号化装置鍵ＣＫＣで暗号化されたコンテンツ鍵ＣＫＭであるＣＫＣ（ＣＫＭ）の受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【００６３】また、デジタルコンテンツ流通業者装置９から復号装置５０への利用許諾情報ＬＭ、許諾電子署名ＳＬＭ、暗号化装置鍵ＣＫＣで暗号化されたコンテンツ鍵ＣＫＭであるＣＫＣ（ＣＫＭ）、およびコンテンツ鍵ＣＫＭで暗号化されたコンテンツMであるＣＫＭ（Ｍ）の受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【００６４】更に、復号装置５０からデジタルコンテンツ流通業者装置９への鍵復号履歴Ｈおよび履歴電子署名ＳＨの受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

【００６５】デジタルコンテンツ流通業者装置９から検知装置７への鍵復号履歴Ｈおよび履歴電子署名ＳＨの受け渡しは、ネットワーク上の通信またはフロッピーディスクやフラッシュメモリカードなどのような汎用的なデジタル情報記録媒体の運搬によって行われるが、本実施形態ではネットワーク上の相互認証通信を用いるものとする。

19

【００６６】次に、以上のように構成される本実施形態のデジタルコンテンツ流通における著作権保護システムの作用について図２内に示すステップ番号Ｓ３１～Ｓ５９を参照して説明する。

【００６７】まず、許諾発行装置１０は、暗号化装置３０からの音楽デジタルコンテンツＭに対する利用許諾情報ＬＭの発行要求に応答して該利用許諾情報ＬＭを発行する（ステップＳ３１）。それから、許諾発行装置１０は、当該許諾発行装置１０内に隠蔽された秘密情報鍵ＣＫＳおよび許諾発行装置秘密鍵ＳＫＬを用いて、利用許諾情報ＬＭに対する許諾電子署名ＳＬＭを生成する（ステップＳ３３）。

【００６８】次に、暗号化装置３０は、前記デジタルコンテンツＭに固有のコンテンツ鍵ＣＫＭを生成する（ステップＳ３５）。それから、暗号化装置３０は、このコンテンツ鍵ＣＫＭを用いて、デジタルコンテンツＭを暗号化して、ＣＫＭ（Ｍ）を生成する（ステップＳ３７）。また、暗号化装置３０は、当該暗号化装置３０内に隠蔽された秘密情報鍵ＣＫＳで暗号化された暗号化装置鍵ＣＫＣであるＣＫＳ（ＣＫＣ）を用いて、前記コンテンツ鍵ＣＫＭを暗号化して、ＣＫＣ（ＣＫＭ）を生成する（ステップＳ３９）。

【００６９】次に、デジタルコンテンツ流通業者装置９は、前記利用許諾情報ＬＭ、許諾電子署名ＳＬＭ、暗号化装置鍵ＣＫＣで暗号化されたコンテンツ鍵ＣＫＭであるＣＫＣ（ＣＫＭ）、コンテンツ鍵ＣＫＭで暗号化されたコンテンツＭであるＣＫＭ（Ｍ）を収集し、これらをネットワークを介して復号装置５０に配送する（ステップＳ４１）。

【００７０】復号装置５０は、前記利用許諾情報ＬＭ、許諾電子署名ＳＬＭ、および許諾発行装置１０と共有する許諾発行装置公開鍵ＰＫＬを用いて利用許諾情報ＬＭの改竄を検知する（ステップＳ４３）。この検知処理において利用許諾情報ＬＭの改竄が検知されない場合には、暗号化装置鍵ＣＫＣで暗号化されたコンテンツ鍵ＣＫＭであるＣＫＣ（ＣＫＭ）を当該復号装置５０内に隠蔽された秘密情報鍵ＣＫＳで暗号化された暗号化装置鍵ＣＫＣであるＣＫＳ（ＣＫＣ）で復号して、コンテンツ鍵ＣＫＭを生成する（ステップＳ４５）。そして、このコンテンツ鍵ＣＫＭの復号時に連続した自然数を履歴通し番号ＮＬとして含む鍵復号履歴Ｈを生成する（ステップＳ４７）。

【００７１】また、復号装置５０は、当該復号装置５０内に隠蔽された秘密情報鍵ＣＫＳで暗号化された復号装置秘密鍵ＳＫＤであるＣＫＳ（ＳＫＤ）を用いて、前記鍵復号履歴Ｈに対する履歴電子署名ＳＨを生成し（ステップＳ４９）、更に鍵復号履歴Ｈに含まれている履歴通し番号ＮＬを当該復号装置５０内に隠蔽する秘密情報鍵ＣＫＳで暗号化してＣＫＳ（ＮＬ）を生成し、暗号化された最後の履歴通し番号ＣＫＳ（ＮＬ）として保持する

20

（ステップＳ５１）。復号装置５０は、コンテンツ鍵ＣＫＭで暗号化されたデジタルコンテンツＭであるＣＫＭ（Ｍ）をステップＳ４５で復号されたコンテンツ鍵ＣＫＭを用いて利用許諾情報ＬＭの定義する許諾範囲に従って復号して、デジタルコンテンツＭを生成する（ステップＳ５３）。

【００７２】次に、デジタルコンテンツ流通業者装置９は、復号装置５０から鍵復号履歴Ｈおよび履歴電子署名ＳＨを収集して、データベース９ａに格納する（ステップＳ５５）。

【００７３】それから、検知装置７は、デジタルコンテンツ流通業者装置９から受け取った鍵復号履歴Ｈおよび履歴電子署名ＳＨ、および復号装置５０と共有している復号装置公開鍵ＰＫＤを用いて、鍵復号履歴Ｈの改竄を検知する（ステップＳ５７）。また、検知装置７は、鍵復号履歴Ｈおよびその前後の鍵復号履歴が含む履歴通し番号の連続性および復号装置５０に保持している履歴通し番号ＮＬを参照して、鍵復号履歴Ｈの不正な抜き取りおよび不正な追加を検知する（ステップＳ５９）。

【００７４】上述したように、音楽デジタルコンテンツＭを利用許諾情報ＬＭの定める許諾範囲内でのみ利用可能とし、この許諾範囲を逸脱したデジタルコンテンツＭの不正利用を検知し、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができる音楽デジタルコンテンツ流通サービスを実現することができる。

【００７５】なお、上記実施形態において、許諾発行装置１０、暗号化装置３０、復号装置５０のいずれかで秘密情報鍵ＣＫＳを用いる代わりに、図１の実施形態で説明したタンパフリー性ハードウェアであるＩＣカードを接続して構成される著作権保護システムを実現することも可能であることは明らかなことである。すなわち、許諾発行装置１０、暗号化装置３０、復号装置５０のうちいずれかの１つまたは２つが秘密情報鍵ＣＫＳを用いる代わりに、図１に示したように演算機能や記憶機能で分割し、この機能を有するタンパフリー性ハードウェアであるＩＣカードを接続して構成してもよいものである。

【００７６】なお、上述した各実施形態では、コンテンツが音楽デジタルコンテンツＭである場合について説明したが、本発明はこのような音楽デジタルコンテンツに限定されるものでなく、その他のコンテンツにも適用可能なものである。

【００７７】

【発明の効果】以上説明したように、本発明によれば、許諾発行装置はデジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行し、利用許諾情報に対する許諾電子署名を生成し、復号装置は許諾発行装置公開鍵および許諾電子署名により利用許諾情報の不正改竄を検知するとともに、暗号化されたコンテンツを利用許諾情報の定義する許諾範囲に従って復号するので、デジタル

コンテンツを許諾範囲内のみで利用可能とし、許諾範囲を逸脱した不正利用を検知して防止することができ、またネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という従来の問題を解決できる。また、復号装置は復号時に許諾発行装置などの外部と接続されている必要がない。

【００７８】また、本発明によれば、検知装置は復号装置公開鍵および鍵復号履歴に付加された履歴電子署名により鍵復号履歴の不正改竄を検知し、鍵復号履歴に含まれる履歴通し番号の連続性および復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知するので、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができ、またコンテンツ利用後の利用履歴抜き取りまたは改竄によるデジタルコンテンツの不正利用を検知して防止できる。更に、検知装置による鍵復号履歴の収集は復号時である必要はなく、復号装置は復号時に検知装置に接続されている必要がない。

【００７９】更に、本発明によれば、許諾発行装置はデジタルコンテンツに対して許諾範囲を定義した利用許諾情報を発行し、利用許諾情報に対する許諾電子署名を生成し、暗号化装置はコンテンツ鍵を生成してコンテンツを暗号化し、コンテンツ鍵を暗号化し、復号装置は許諾発行装置公開鍵および利用許諾情報に付加された許諾電子署名により利用許諾情報の不正改竄を検知し、暗号化されたコンテンツ鍵を復号し、この復号時に連続した履歴通し番号を含む鍵復号履歴を生成し、鍵復号履歴に履歴電子署名を付加し、暗号化されたデジタルコンテンツを利用許諾情報の定義する許諾範囲に従って復号し、検知装置は復号装置公開鍵および鍵復号履歴に付加された履歴電子署名により鍵復号履歴の不正改竄を検知し、鍵復号履歴に含まれる履歴通し番号の連続性および復号装置に保持している履歴通し番号の参照により鍵復号履歴の不正な抜き取りおよび不正な追加を検知するので、デジタルコンテンツを許諾範囲内のみで利用可能とし、許諾範囲を逸脱した不正利用を検知して防止することができ、デジタルコンテンツ流通業者の水増し請求やデジタルコンテンツ利用者の利用否認による支払い拒否などを防止することができるとともに、コンテンツ利用後の利用履歴抜き取りまたは改竄によるデジタルコンテンツの不正利用を検知して防止でき、またネットワーク上の相互認証通信によるトラヒックの増加およびサービスコストの増加、ネットワーク非接続時のコンテンツ利用不可という従来の問題を解決できる。

【００８０】本発明によれば、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリー性ハードウェア内に閉じて実行するので、暗号化装置のセキュリティを高め、その不正防止効果を向上することができる。

【００８１】また、本発明によれば、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与をタンパフリー性ハードウェア内に閉じて実行するので、許諾発行装置のセキュリティを高め、その不正防止効果を向上することができる。

【００８２】更に、本発明によれば、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行するので、復号装置のセキュリティを高め、その不正防止効果を向上することができる。

【００８３】本発明によれば、暗号化装置、許諾発行装置、および復号装置は秘密情報鍵を共有し、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００８４】また、本発明によれば、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリー性ハードウェア内に閉じて実行し、許諾発行装置および復号装置は秘密情報鍵を共有し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００８５】更に、本発明によれば、許諾発行装置は許諾発行装置秘密鍵保持手段および許諾電子署名生成付与をタンパフリー性ハードウェア内に閉じて実行し、暗号化装置および復号装置は秘密情報鍵を共有し、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００８６】本発明によれば、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行し、暗号化装置および許諾発行装置は秘密情報鍵を共有し、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００８７】また、本発明によれば、暗号化装置は暗号化装置鍵を秘密情報鍵で暗号化して保持し、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与をタンパフリー性ハードウェア内に閉じて実行し、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００８８】更に、本発明によれば、許諾発行装置は許諾発行装置秘密鍵を秘密情報鍵で暗号化して保持し、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリー性ハードウェア内に閉じて実行し、復号装置は鍵保持、利用許諾情報不正改竄検知、コンテンツ鍵復号、鍵復号履歴生成、履歴通し番号保持、履歴電子署名付加をタンパフリー性ハードウェア内に閉じて実行するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【００８９】本発明によれば、復号装置は暗号化装置鍵、復号装置秘密鍵、履歴通し番号を秘密情報鍵で暗号化して保持し、暗号化装置はコンテンツ鍵生成、コンテンツ鍵暗号化、および暗号化装置鍵保持をタンパフリー性ハードウェア内に閉じて実行し、許諾発行装置は許諾発行装置秘密鍵保持および許諾電子署名生成付与をタンパフリー性ハードウェア内に閉じて実行するので、暗号化装置、許諾発行装置、および復号装置のそれぞれのセキュリティを高め、その不正防止効果を向上することができる。

【図面の簡単な説明】

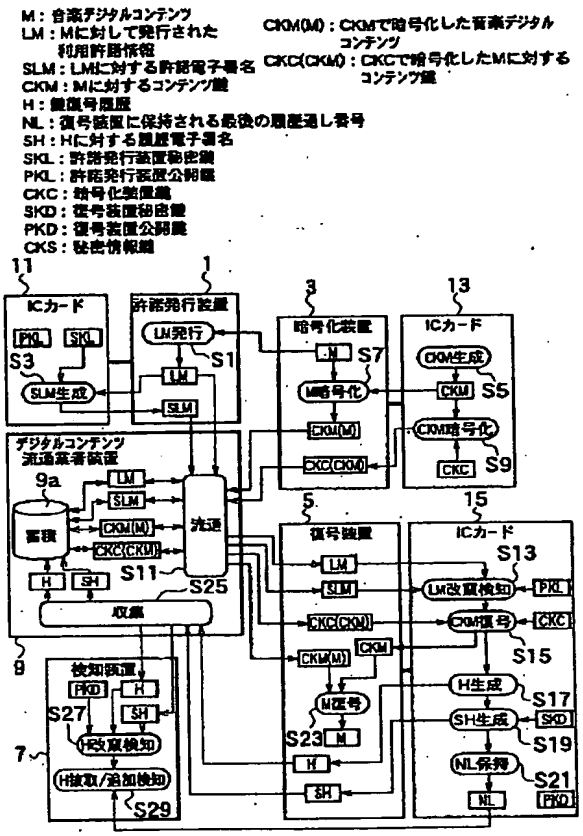
【図１】本発明の一実施形態に係るデジタルコンテンツ流通における著作権保護システムの構成を示す図である。

【図２】本発明の他の実施形態に係るデジタルコンテンツ流通における著作権保護システムの構成を示す図である。

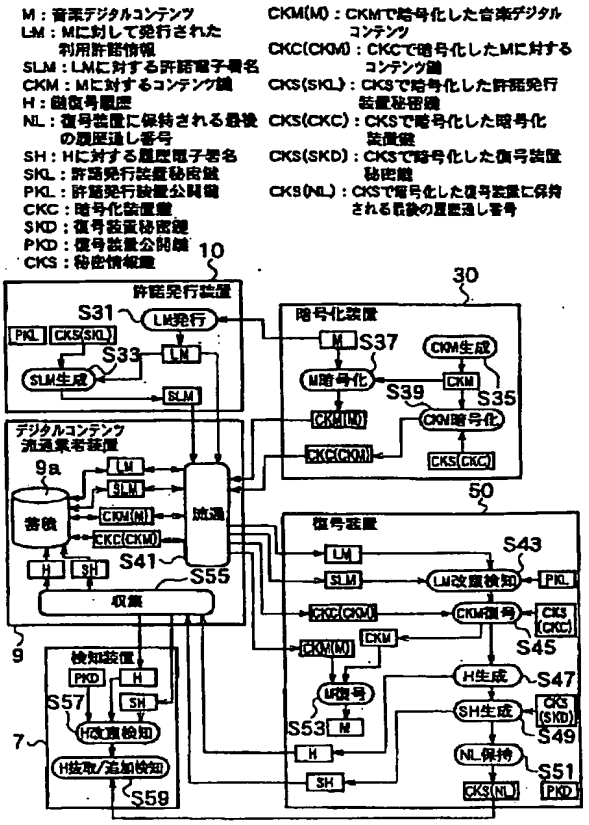
【符号の説明】

１，１０　許諾発行装置
３，３０　暗号化装置
５，５０　復号装置
７　検知装置
９　デジタルコンテンツ流通業者装置
１１　許諾発行装置用ＩＣカード
１３　暗号化装置用ＩＣカード
１５　復号装置用ＩＣカード

【図１】



【図２】



フロントページの続き

(51) Int. Cl.⁷	識別記号	F I	テーマコード（参考）
Ｇ０６Ｋ　19/10		Ｇ０６Ｋ　19/00	Ｒ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ

Ｆターム（参考）　5B017 AA03 AA06 AA08 BA07 BA09 CA14
5B035 AA13 BB09 BC00 CA11
5B058 CA27 KA02 KA04 KA08 KA31 KA35 YA20
5J104 AA09 LA03 LA06 NA02 NA35 NA42